ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

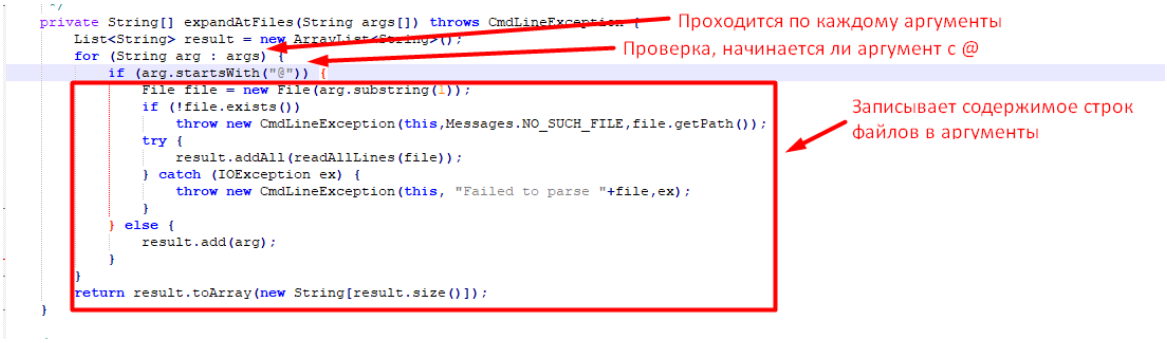

Рисунок 8. Метод expandAtFiles()

Метод **expandAtFiles**(String args[]) проходит по всем элементам массива args. Если элемент начинается с символа '**@**', то метод пытается прочитать файл, указанный в этом элементе, и заменить элемент массива на строки из этого файла, тем самым выводя содержимое произвольного файла, неаутентифицированному пользователю, что и было продемонстрировано в примерах эксплуатации выше.

Метод expandAtFiles() является небезопасным и представляет главную причину возникновения уязвимости произвольного чтения файлов в Jenkins CVE-2024-23897.

Рекомендации по устранению

Обновите Jenkins до версии, начиная с Jenkins 2.442, LTS 2.426.3 и LTS 2.440.1. В этих версиях функция синтаксического анализатора команд отключена, что предотвращает замену символа @ на содержимое файла для команд CLI в аргументах, и тем самым устраняет уязвимость произвольного чтения файлов CVE-2024-23897.

Вывод

Актуальный анализ уязвимости CVE-2024-23897 подчеркивает важность регулярной проверки и обновления зависимостей третьих сторон в информационных системах. Уязвимость, обусловленная использованием устаревшей библиотеки (args4j), подтверждает, что сторонние приложения могут стать ключевым источником слабых мест и угроз в системах. Этот инцидент подчеркивает необходимость активного мониторинга обновлений безопасности в используемых библиотеках и приложениях. Регулярное обновление зависимостей и внимательное отслеживание обновлений помогут предотвратить подобные уязвимости и улучшить общий уровень кибербезопасности.

Список использованных источников

1. National Vulnerability Database (NVD): CVE-2024-23897 Detail. – URL: https://nvd.nist.gov/vuln/detail/CVE-2024-23897 (дата обращения: 16.03.2024)

2. Common Vulnerabilities and Exposures (CVE): CVE-2024-23897. – URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23897 (дата обращения: 16.03.2024)

3. Jenkins Documentation. – URL: https://www.jenkins.io/doc/ (дата обращения: 16.03.2024)

4. Args4j: Java Command-Line Parser Library by Kohsuke Kawaguchi. – URL: https://args4j.kohsuke.org/ (дата обращения: 16.03.2024)

УДК 512.647

МОБИЛЬДІ ҚҰРЫЛҒЫЛАРҒА АРНАЛҒАН ҚҰПИЯ СӨЗ ҚОСЫМШАЛАРЫН ӘЗІРЛЕУДЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІК БОЙЫНША ҰСЫНЫСТАР

Сүлеймен Әлихан Қайратұлы
asuleimenov.21@gmail.com

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті «7М06306 – Ақпараттық қауіпсіздік жүйелері» білім беру бағдарламасының 1-курс магистранты, Астана, Қазақстан
Ғылыми жетекші – Ташенова Ж.М.

Аннотация. Бұл мақалада мобильді қосымшалар үшін құпия сөз реттеушілерін әзірлеу әдістері мен үздік тәжірибелеріне толық шолу берілген. Зерттеулер мен ұсыныстарға, сондай-ақ нарықтағы бар шешімдерге талдау жүргізіліп құпия сөз қауіпсіздігінің негізгі аспектілері, құпия сөздерді сақтау және жасау әдістері, сондай-ақ деректер мен пайдаланушы тіркелгілерін қорғау стратегиялары қарастырылады. Сонымен қатар, мақалада пайдаланушы интерфейсі мен ыңғайлылық мәселелері талқыланады және деректер қауіпсіздігін жақсарту үшін дизайн принциптері мен тиімді құпия сөзді басқаруды ұстанудың маңыздылығына баса назар аударылады.

Кілт сөздер: Құпия сөз менеджерлері, мобильді қолданбалар, ақпараттық қауіпсіздік, шифрлеу, хэштеу.

Кіріспе. Мобильді құрылғылар күнделікті өміріміздің ажырамас бөлігіне айналып жатқандықтан әлемде жеке деректердің қауіпсіздігін қамтамасыз ету басымдық болып табылады. Технологияның дамуымен және онлайн қызметтер санының өсуімен пайдаланушылар бірнеше тіркелгілер мен құпия сөздерді басқару қажеттілігіне тап болды. Осы қажеттілікке жауап ретінде құпия сөздерді сақтау мен пайдаланудың ыңғайлы және қауіпсіз әдісін ұсынатын мобильді құрылғыларға арналған құпиясөз менеджерлері пайда болуда.

Мобильді қолданбаларға арналған құпия сөз реттеушісін зерттеу және әзірлеу құпия сөзді сақтаудың қауіпсіз әдістерінен пайдаланушыға ыңғайлы және интуитивті пайдаланушы интерфейсін құруға дейінгі тақырыптардың кең ауқымын қамтиды.

Негізгі аспектілерге құрылғыда құпия сөздерді сақтау қауіпсіздігін қамтамасыз ету үшін деректерді шифрлау механизмдерін әзірлеу, сондай-ақ осалдықтарды болдырмау үшін күшті құпия сөздерді генерациялау алгоритмдерін әзірлеу кіреді.

Сонымен қатар, қолданбалар мен браузерлерде құпия сөзді автоматты түрде толтыру, құрылғылар арасында деректерді синхрондау және басқа қызметтермен біріктіру сияқты ыңғайлылық аспектілеріне маңызды көңіл бөлінеді.

Сондай-ақ қолданбаның өнімділігін оңтайландыру және ықтимал қауіпсіздік шабуылдарынан қорғауды қамтамасыз ету сияқты тәжірибелік даму аспектілеріне назар аудару маңызды.

Нәтижесінде, мобильді қосымшаларға арналған құпия сөз реттеушісін зерттеу және әзірлеу – пайдаланушылардың жеке деректерін сенімді қорғауды қамтамасыз ету үшін қауіпсіздіктің, ыңғайлылықтың және функционалдылықтың әртүрлі аспектілерін ескеруді талап ететін күрделі процесс.

Құпия сөздерді қауіпсіз сақтау әдістері. Құпия сөздердің қауіпсіз сақталуын қамтамасыз ету мобильді құрылғылар үшін құпия сөз реттеушісін әзірлеу кезінде маңызды аспект болып табылады. Пайдаланушы құпия сөздерінде құпия ақпарат бар, сондықтан оларды сақтау қауіпсіз болуы керек.

Ең кең таралған әдістердің бірі - құпия сөздерді дерекқорда сақтамас бұрын хэштеу. Бұл процесс құпия сөзді SHA-256 немесе bcrypt сияқты криптографиялық алгоритмдер арқылы хэш мәніне түрлендіру болып табылады. Алынған хэш мәні құпия сөздің орнына дерекқорда сақталады. Бұл әдіс қосымша қауіпсіздік деңгейін қамтамасыз етеді, себебі дерекқор бұзылса да, шабуылдаушыға бастапқы құпия сөздерді қалпына келтіру қиын болады.

Басқа әдіс – асимметриялық шифрлауды қолдану. Құпия сөздерді ашық кілт арқылы шифрлауға, содан кейін серверде сақтауға болады. Дегенмен, құпия сөздердің шифрын шешу үшін тек серверде сақталатын жеке кілт қажет. Бұл қосымша қауіпсіздік деңгейін қамтамасыз

етеді, себебі дерекқор қол жетімді болса да, шабуылдаушы жеке кілтсіз бастапқы құпия сөздерге қол жеткізе алмайды.

Құпия сөздерді қорғаудың қосымша әдісі - оларды тұздау(орыс тілінде – “использование соли”). Бұл процесс құпия сөзге хэштеу алдында кездейсоқ жолды қосуды қамтиды. Бұл құпия сөздерді бірегей етеді және шабуылдаушы дерекқорға қол жеткізе алса да, бұзуды қиындатады.

Сенімді құпия сөздерді құру алгоритмдері. Сенімді құпия сөздерді жасау пайдаланушы тіркелгілерінің қауіпсіздігін қамтамасыз етудің ажырамас аспектісі болып табылады. Бұл мақсатта қауіпсіздіктің жоғары стандарттары ескеріледі. Жалпы әдістердің бірі - берілген ұзындықтағы кездейсоқ таңбаларды пайдаланып құпия сөздерді жасау. Бұл тәсіл пайдаланушылар үшін қауіпсіздіктің жоғары деңгейін қамтамасыз ететін әдіс. Ол шабуылға төзімді құпия сөздердің жасалуын қамтамасыз етеді.

Бұған қоса, құпия сөз ретінде бірнеше сөздерді немесе сөздердің кездейсоқ комбинацияларын пайдалануды ұсынатын құпия сөз тіркестерін құру тәсілі бар. Мұндай құпия сөздер шабуылдарға өте төзімді және пайдаланушыларға есте сақтауға оңай.

Сондай-ақ белгілі бір қызметтердің немесе жүйелердің құпия сөз талаптарын ескеру маңызды. Кейбір қызметтерде құпия сөздің минималды ұзындығына немесе белгілі бір таңба түрлерін пайдалануына арнайы талаптары болуы мүмкін. Сондықтан қауіпсіздік пен қызметтің стандарттарына сәйкестігін қамтамасыз ету үшін құпия сөздерді жасау кезінде осы талаптарды ескеру маңызды.

Деректерді құрылғылар арасында синхрондау. Құпия сөз реттеушісінің ыңғайлылығы оны пайдаланушылар қабылдауында маңызды рөл атқарады. Қолданбаның пайдаланушы интерфейсін құрастырған кезде интуитивтік пен пайдаланудың қарапайымдылығына ерекше назар аудару керек. Мысалы, қолданба сақталған тіркелгі деректерін қосу, өңдеу және басқару үшін оңай, түсінікті құралдармен қамтамасыз етілуі керек.

Қолдану мүмкіндігін жақсартудың бір жолы - қолданбалар мен браузерлерде құпия сөздерді автоматты түрде толтыру. Бұл пайдаланушыларға сақталған тіркелгі деректерін пайдаланып кіру пішіндерін оңай толтыруға мүмкіндік береді. Сонымен қатар, қолданба деректерді құрылғылар арасында синхрондау мүмкіндігін қамтамасыз етуі керек. Бұл функция арқылы пайдаланушыда құпия сөз бен тіркелгі деректері кез-келген құрылғыдан қолжетімді болады.

Пайдаланушыларға ыңғайлы болу үшін сақталған деректерге оңай және жылдам қол жеткізуді қамтамасыз ету де маңызды. Мысалы, саусақ ізі сканері немесе бет-әлпетті тану сияқты биометриялық аутентификация әдістерін пайдалану, жүйеге кіру процесін айтарлықтай жеңілдетеді. Сондай-ақ, қолданбада желіден тыс режимде жұмыс істеу мүмкіндігі болуы керек, бұл пайдаланушыларға Интернетке қосылмаған жағдайда өздерінің тіркелгілеріне қол жеткізуге мүмкіндік береді.

Жалпы мақсат - қауіпсіздіктің жоғары деңгейін қамтамасыз етіп қана қоймай, сонымен қатар құпия сөздер мен тіркелгі деректерін басқаруға ыңғайлы және интуитивті құралдарды ұсынатын қолданбаны жасау.

Қолданбаны оңтайландыру және шабуылдан қорғау. Мобильді қосымшалар үшін құпия сөз реттеушісін әзірлеу кезінде өнімділікті оңтайландыру және ықтимал шабуылдардан қорғау маңызды аспектілер болып табылады. Қосымша жылдам және құрылғы ресурстарын тиімді тұтынуы керек. Бұл жад пен процессордың пайдалануын оңтайландыруды, сондай-ақ деректерді жүктеу уақытын азайту үшін желілік сұрауларды оңтайландыруды қамтиды.

Мүмкін шабуылдардан қорғау үшін осалдықтарды анықтау және алдын алу қажет. Мысалы, желілік трафикті бақылау, бұзу әрекетін көрсетіп, мүмкін аномальды әрекетті анықтауға көмектеседі. Сондай-ақ, хакерлердің оны ұстап алуына жол бермеу үшін деректер желі бойынша қозғалған кезде шифрланғанын қамтамасыз ету маңызды.

Оған қоса, анықталған осалдықтарды түзету және шабуылдардан қорғауды жақсарту үшін қолданбаны және оның құрамдастарын үнемі жаңартып отыру керек. Қосымшаны

жаңартып отыру оның соңғы қауіпсіздік стандарттарына сәйкес келуіне және пайдаланушыларды жаңа қауіптерден қорғауға көмектеседі.

Қорытынды. Мақалада айтылып кеткен деректерге сүйенетін болсақ, қауіпсіздік назар аударуды қажет ететін жалғыз аспект емес. Құпия сөз менеджерін әзірлеуде пайдаланушы тәжірибесі де маңызды рөл атқарады. Әзірлеушілер пайдаланушыларға тіркелгі деректерін оңай басқаруға және қажетті ақпаратқа қол жеткізуге мүмкіндік беретін интуитивті және қолдануға оңай интерфейс жасауға ұмтылуы керек.

Сонымен қатар, пайдаланушыларды ақпараттық қауіпсіздік негіздерімен таныстыру жалпы қауіпсіздікті жақсартуда маңызды рөл атқарады. Пайдаланушылар құпия сөзді қорғау тәсілдері, әлсіз құпия сөздерді пайдалану қаупі және олардың тіркелгілеріне шабуылдардың алдын алу әдістері туралы білім алуы керек. Тұрақты ақпараттық науқандар мен оқу материалдары пайдаланушылардың хабардарлығын арттыруға және онлайн ортаны барлығы үшін қауіпсіз етуге көмектеседі.

Сонымен, мақаланың қорытындысында қауіпсіз құпия сөз менеджерлерін әзірлеудің техникалық аспектілері ғана емес, сонымен қатар мобильді қосымшаларда тіркелгі деректерін тиімді және қауіпсіз пайдалануды қамтамасыз ететін пайдаланушылардың рөлін түсіну және оларды оқыту маңыздылығына баса назар аударылады.

Пайдаланылған әдебиеттер тізімі

1. Ayyagari R. Why Do Not We Use Password Managers? A Study on the Intention to Use Password Managers / R. Ayyagari // Contemporary Management Research. 2019. P. 227–245.
2. Bahmanziari T.P. Is Trust Important in Technology Adoption? A Policy Capturing Approach / T.P. Bahmanziari // Journal of Computer Information Systems. 2003. № 43(4). P. 46–54
3. "Безопасность мобильных приложений" Гупта, Химаншу (2019). P. 127–144
4. "Руководство хакера веб-приложений: Поиск и использование уязвимостей" Статтард, Дафидд и Пинто, Маркус (2014).
5. Разработка менеджера паролей под Android. https://habr.com/ru/articles/328708/

УДК 004.056

ИССЛЕДОВАНИЕ КИБЕРУГРОЗ ДЛЯ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ ДЕЯТЕЛЬНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУР

Тұрарғазинов Жандос Серікқазыұлы
turargazinov_zhs@enu.kz
Магистрант Евразийского национального университета им. Л. Н. Гумилева,
Астана, Казахстан
Научный руководитель-к.ф-м.н., ассоциированный профессор, Сатыбалдина Д.Ж.

Аннотация

В данной статье осуществляется комплексный анализ киберугроз, с которыми сталкиваются критически важные инфраструктуры Республики Казахстан. Особое внимание уделяется идентификации основных типов кибератак, в частности, доминирующему влиянию фишинговых операций, и их воздействию на непрерывность функционирования жизненно важных секторов экономики и социальной сферы. В работе представлен обзор текущего состояния кибербезопасности в стране, включая анализ недавних инцидентов и мер реагирования на них. Основываясь на международном опыте и текущих тенденциях, предложены конкретные стратегии и решения для укрепления киберустойчивости критически важных инфраструктур Казахстана. Рекомендации включают разработку и внедрение национальных стандартов кибербезопасности, обучение и повышение осведомленности сотрудников, усиление межведомственного и международного сотрудничества, применение современных технологий защиты и разработку планов реагирования на инциденты. Статья подчеркивает необходимость комплексного подхода к обеспечению кибербезопасности,